MIGRATION FROM IN-CLEAR TO ENCRYPTED WORKING OVER A COMMUNICATIONS LINK

Abstract

A system involving a central computer (2) and a remote computer (3), which can communicate over a link (1), is migrated from in-clear working to encrypted working automatically as the computers receive and install long term keys necessary for encrypted communication. When migration is required, the settings at both ends of the link need to be changed to "encrypt" simultaneously and, particularly, if there are numerous remote computers and the possibility of connection of a remote computer to different central computers, as is possible in virtual private network (VPN) scenarios, severe problems can ensue. Hence, as well as the normal two modes of working "in-clear" and "encrypt", a third mode in which "initiate encryption" is set at one end of the link and "accept encryption" is set at the other end of the link. is proposed. This third mode ensures that working in-clear can continue over a particular link, such as between a particular VPN server and a particular gateway PC, until a long term key required for encrypted working is installed at both ends of the link, but that once key installation is complete, only encrypted working is possible over that link.